

IMPLEMENTASI NETWORK ACCESS PROTECTION PADA JARINGAN WIRELESS

Dosen Pembimbing I : Basuki Rahmat, S.si, MT
Dosen Pembimbing II : Crystia Aji Putra, S.Kom
Penyusun : Fajar Bangkit Sutomo

ABSTRAK

Dengan semakin majunya perkembangan teknologi tentunya di ikuti oleh perkembangan yang positif dan negatif.

Makin mudahnya mendapat akses internet membuat masyarakat atau mahasiswa sudah mengetahui tentang dampak negatif dari akses internet itu diantaranya adalah situs porno dan banyak virus berjalan didalam jaringan.

Karena itu Tugas akhir ini akan membahas tentang tahap-tahap implementasi network access protection pada jaringan wireless untuk fakultas teknik informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur. Metodologi yang bisa digunakan dalam pembuatan system ini adalah analisa berbasis opensorce dan antivirus proxy.

Manfaat dari tugas akhir ini adalah terciptanya sebuah jaringan yang bersih dan terjaga di fakultas teknik informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.

Kata Kunci : network access protection, wireless, opensource.

DAFTAR ISI

ABSTRAK	i
KATA PENGANTAR	ii
DAFTAR ISI	vi
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
BAB I PENDAHULUAN	
1.1. Latar Belakang.....	1
1.2. Perumusan Masalah	2
1.3. Batasan masalah	3
1.4. Tujuan dan Manfaat	3
1.5. Metodologi Penelitian	4
1.6. Sistematika penulisan.....	6
BAB II TINJAUAN PUSTAKA	
2.1. Netwok Access Protection.....	8
2.2. Metode Access Protection.....	10

2.3.	Peraturan Keamanan Firewall	11
2.3.1	Karakteristik Firewall.....	11
2.3.2	Teknik Yang Digunakan Firewall.....	12
2.3.3	Mengenal Iptables.....	13
2.3.4	Perizinan Sesi Sambungan Yang Terbentuk.....	13
2.4.	Mengenal virus komputer.....	16
2.5.	Mengenal Ruoter.....	19
2.5.1	Mengenal Dhcp Server	20
2.6.	Mengenal Squid Web Proxy.....	21
2.7.	Mengenal havp Antivirus proxy.....	23
2.8.	Mengenal jaringan wireless.....	23
2.8.1	Wireless LAN	24
2.8.2	Mode Pada Wireless LAN.....	24
2.8.3	Komponen Pada Wlan	25

BAB III TINJAUAN PUSTAKA

3.1.	Analisa Sistem.....	27
3.2	Perancangan Sistem	29
3.3	Deskripsi Umum Sistem.....	30
3.4	Skema mekanisme dan cara kerja.....	32

3.5 Flowchart Proses Network Access Protection.....	33
---	----

BAB IV ANALISA DAN PERANCANGAN SISTEM

4.1. Installasi Router	34
4.1.1. Install Paket DHCP Server.....	36
4.2. Membuat Anti Virus Proxy.....	38
4.3. Kemampuan havp.....	45
4.4. Merubah tampilan havp.....	47
4.5 Membuat koneksi wireless.....	48
4.5 Pedeteksian Client Menggunakan Nmap.....	52
4.6 Menutup Port Masuknya Virus	55
4.7 Pembatasan Hak Akses Client.....	56

BAB V UJI COBA DAN EVALUASI

5.1. Minimum hardware uji coba network access protection.....	58
5.2. Uji Coba Router.....	59
5.3 Uji Coba Mengubah Semua Akses Ke Port 3128.....	62
5.4 Uji Coba Koneksi Wireless	63
5.5 Uji Coba koneksi wireless di client.....	64
5.6 Uji Coba Client havp Antivirus Proxy	67

5.7 Uji Coba blokir virus dengan havp	69
5.8 Uji Coba Blokir Situs dengan Havp.....	69
5.9 Uji Coba Deteksi Alamat Ip Clien	70
5.10 Uji Coba Deteksi Port Service	71
5.11 Uji Limited Client	73

BAB VI PENUTUP

6.1 Kesimpulan.....	76
6.2 Saran.....	77

DAFTAR PUSTAKA	78
----------------------	----

LAMPIRAN

DAFTAR GAMBAR

Gambar 2.1 Nap pada windows server 2008.....	9
Gambar 2.1 Cara kerja firewall	11
Gambar 3.1 Skema dan cara kerja.....	32
Gambar 4.1 Tampilan media jaringan yang terdeteksi	36
Gambar 4.2 Cara install havp.....	38
Gambar 4.3 Cara install squid	39
Gambar 4.4 Cara install clamav antivirus.....	39
Gambar 4.5 Cara install clamav daemon yaitu plugin dari anti virus	40
Gambar 4.6 Update antivirus clamav.....	40
Gambar 4.7 Pengaturan squid agar dapat membaca havp.	41
Gambar 4.8 Pengaturan squid agar dapat membaca proxy.	42
Gambar 4.9 Pengaturan agar setiap access yang lewat melalui port 3128. ..	43
Gambar 4.10 Blokir virus	44
Gambar 4.11 Tampilan havp untuk blokir situs.....	45
Gambar 4.12 Tampilan menambahkan blokir situs.....	46
Gambar 4.13 pengaturan kartu jaringan untuk membuat akses wireless.....	49

Gambar 4.14 melakukan pengaturan kartu jaringan.....	50
Gambar 4.15 koneksikan kartu jaringan.....	50
Gambar 4.16 profile yang terdeteksi dan berhasil dibuat.....	51
Gambar 4.17 pengaturan alamat ip dari jaringan wireless.....	51
Gambar 4.13 Tampilan scanning port jika firewall client hidup.....	53
Gambar 4.14 Tampilan scanning jika firewall client tidak hidup.	53
Gambar 4.15 Tampilan scaning ip client yang sedang aktif.....	54
Gambar 4.16 Tampilan dari /etc/rc.local.....	56
Gambar 5.1 hilangnya kartu jaringan yang dimiliki router.....	59
Gambar 5.2 Pengaturan kartu jaringan router.....	60
Gambar 5.3 Mengatasi kartu jaringan yang hilang.....	60
Gambar 5.4 kartu jaringan yang sudah terdeteksi	61
Gambar 5.5 Menghidupkan dhcp server.....	62
Gambar 5.6 Pengaturan iptables redirect ke port 3128.....	63
Gambar 5.7 jaringan yang terdeteksi router	64
Gambar 5.8 melakukan koneksi jaringan wireless pada sisi client.....	65
Gambar 5.9 jaringan wireless keren dideteksi oleh client.	65
Gambar 5.10 deteksi ip client di windows.....	66
Gambar 5.11 deteksi client di linux.....	67
Gambar 5.12 Pengaturan proxy dari sisi client	68

Gambar 5.13 Tampilan membuka browser tanpa proxy.....	68
Gambar 5.14 Tampilan havp untuk blokir virus.	69
Gambar 5.15 Tampilan havp untuk blokir situs.	70
Gambar 5.16 Tampilan scanning ip client.	71
Gambar 5.17 Tampilan deteksi port service.	72
Gambar 5.18 Tampilan client yang tidak aktifkan firewall.	72
Gambar 5.19 Tampilan client yang aktifkan firewall.....	73
Gambar 5.20 menutup koneksi penuh koneksi client.....	74
Gambar 5.21 Tampilan akses yang terputus dari client ke server.....	74

DAFTAR TABEL

Tabel 3.1 Cara kerja network access protection	33
--	----

Tabel 5.1 Minimum Hardware Untuk Menjalankan Network Access Protection.	51
---	----

BAB I

PENDAHULUAN

1.1 Latar Belakang

Media internet telah tersebar ke seluruh dunia, karena internet digunakan sebagai media komunikasi publik yang bersifat terbuka. Maka akses internet sudah banyak ditemui mulai dari kafe-kafe sampai restoran pun menggunakan media internet untuk memberi daya tarik bagi pengunjung biasanya tempat seperti itu memberikan akses internet gratis via wireless kepada pengunjung sehingga pengunjung menambah minat untuk selalu kembali dan berkunjung ke tempat tersebut tetapi semakin banyak pengunjung maka akan mempersulit tugas administrator jaringan untuk mengelola jaringan agar jaringan tetap stabil dan koneksi internet tidak terganggu oleh masalah virus yang dapat mengganggu koneksi jaringan untuk itu seorang administrator jaringan harus menjaga akses computer yang akan menggunakan jaringan, agar stabilitas internet tetap terjaga dan tidak terganggu untuk itu diperlukan sebuah network access protection untuk membantu seorang network administrator untuk menjaga jaringan mereka dari serangan virus, spyware atau aplikasi jahat lainnya.

Network Access Protection (NAP) memberikan kemampuan kepada enterprise control total terhadap keamanan system melalui suatu mekanisme Karantina dan Health Checking System yang terintegrasi dengan group policy yang pada akhirnya memberikan total compliance.

Hal inilah yang menjadikan NAP sebagai compliance enforcer, yang mampu menjaga security compliance dengan melakukan enforce security policy kepada seluruh user didalam lingkup sistem tersebut, NAP dapat menjaga betapa “kotornya” device yang masuk ke dalam sistem, kemanan sistem dan security compliance bisa selalu terjamin.

1.2` Perumusan Masalah

Seperti yang kita ketahui bersama masalah virus didalam jaringan internet sangat mengganggu kita mulai dari melambatnya akses internet yang kita miliki sampai merusak sistem operasi yang kita miliki untuk itu diperlukan network access protection yang dapat menjaga jaringan internet agar terhindar dari virus, spyware, atau program jahat lainnya permasalahan lain yang timbul dari penelitian ini adalah :

1. Bagaimana mengatur Health Policy Validation agar dapat menentukan apakah tingkat keamanan komputer klien sudah sesuai dengan standar kebijakan keamanan yang dibuat oleh administrator jaringan.
2. Bagaimana mengatur Health Policy Compliance jika akses tidak lolos validasi, maka user tersebut akan dikarantina.
- 3 Automatic Health Recovery agar melakukan scan otomatis pada file yang terdapat virus.
- 4 Limited Access Management agar dapat membatasi akses suatu komputer klien yang tidak memenuhi standar kebijakan keamanan.

1.3 Batasan Masalah

Dari permasalahan yang telah disebutkan di atas, maka batasan-batasan dalam tugas akhir ini adalah :

1. Penelitian ini didasarkan pada studi kasus jurusan teknik informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.
2. Tidak di implementasikan secara real pada jaringan wireless di jurusan teknik informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.
3. Pengerjaan sistem dilakukan dengan aplikasi linux (ubuntu 10.10) dengan aplikasi havp.
4. Pembahasan mengenai aplikasi havp dan firewall.
5. Pembahasan mengenai grup policy management yaitu ketentuan kebijakan manajemen yang ditetapkan oleh administrator.
6. Pembahasan mengenai proteksi terhadap virus pada jaringan internet menggunakan antivirus clamsav dan squid.
7. Pembahasan mengenai proteksi terhadap virus pada jaringan lokal menggunakan firewall.

1.4 Tujuan dan Manfaat

Tujuan yang ingin di capai dari penelitian tugas akhir ini adalah untuk :

1. Membuat sistem jaringan yang terjamin keamanan dan terkendali.
2. Mempermudah seorang network administrator untuk mengatur jaringan.

3. Mengatur jalannya jaringan dengan baik, terjaga dari virus dan aplikasi jahat lainnya.

Dengan melakukan penelitian ini, diharapkan dapat memberikan manfaat diantaranya :

1. Sebagai penambah wawasan dan meningkatkan kemampuan mahasiswa dalam melakukan perubahan teknologi .
2. Dapat membuat sistem jaringan yang aman dan terjaga.
3. Mempermudah seorang network administrator mengatur jaringan.
4. Memiliki akses internet yang terproteksi dari virus maupun aplikasi jahat lainnya.

1.5 Metodologi Penelitian

Dengan kemajuan mobility, seperti PDA , push mail dan sebagainya menambah tantangan dalam menjaga security compliance perusahaan. Hal ini menjadi tantangan yang tersendiri bagi para IT administrator yang bertanggung jawab atas security compliance seluruh karyawan kapan pun, dimanapun dengan media apapun. Hal inilah yang menjadikan NAP sebagai compliance enforcer, yang mampu menjaga security compliance dengan menerapkan security policy kepada seluruh user didalam lingkup sistem tersebut, NAP dapat menjaga betapa “kotornya” device yang masuk ke dalam sistem, keamanan sistem dan security compliance bisa selalu terjamin.

Dalam proposal tugas akhir saya ini, saya angkat implementasi network access protection pada jaringan wireless area network yang dapat digunakan sebagai satu alat IT administrator untuk memenuhi tantangan semakin majunya teknologi saat ini agar keamanan pada jaringan dapat selalu bersih dan terjamin.

Langkah –langkah yang ditempuh untuk menyelesaikan tugas akhir ini antara lain adalah :

a. Studi Literatur

Tahapan untuk memperdalam teori dan mencari referensi-referensi yang berkaitan dengan tema tugas akhir ini. Sumber referensi berasal dari artikel berupa e-book, jurnal, skripsi, thesis, dan buku. Tahapan ini sangat penting karena digunakan untuk menunjang tahapan-tahapan berikutnya dalam penyusunan tugas akhir.

b. Analisa Kebutuhan

Tahapan ini untuk menganalisa apa saja kebutuhan untuk penelitian tugas akhir. Seperti pengumpulan data, analisa data, dan analisa kebutuhan hardware dan software. Tahapan ini sangat penting untuk menunjang pada tahapan perancangan sistem.

c. Perancangan Sistem

Pada tahap ini, dimulainya pembuatan rancangan sistem. Mulai dari desain topologi jaringan, konfigurasi tiap-tiap router dan perancangan sistem agar dapat mencapai tujuan sesuai dengan topik pembahasan. Hasil pada tahapan ini akan dilanjutkan pada tahapan implementasi sistem.

d. Pembuatan Sistem

Pada tahap ini, dilakukan pengimplementasian rancangan yang telah disusun pada tahap sebelumnya sesuai konsep yang telah dibuat. Sistem dapat mengalami perubahan konsep dari rancangan sebelumnya maka pada tahapan ini akan dilakukan perubahan pembuatan sistem sampai mencapai hasil yang diharapkan.

e. Uji Coba Sistem

Pada tahapan ini dilakukan pengecekan apakah sistem memiliki kemampuan seperti yang diharapkan.

f. Pembuatan Kesimpulan

Tahapan ini merupakan tahap akhir setelah sistem telah berjalan seperti yang diharapkan dilakukan evaluasi dan penarikan kesimpulan.

1.6 Sistematika Penulisan

Laporan Tugas Akhir ini akan dibagi mejad beberapa bab, sebagai berikut :

a. Bab I PENDAHULUAN

Berisi Latar Belakang, Tujuan, Permasalahan, Ringkasan isi tugas akhir, batasan masalah, tinjauan pustaka, metodologi dan sistematika penulisan.

b. Bab II TINJAUAN PUSTAKA

Berisi tentang teori dan penjelasan dari metode-metode yang akan digunakan dalam membuat perancangan network access protection pada jaringan wireless.

c. Bab III ANALISIS DAN PERANCANGAN SISTEM

Yang berisi tentang perencanaan, analisis, rancangan, penerapan, dan penggunaan .

d. Bab IV IMPLEMENTASI SISTEM

Pada bab ini menjelaskan tentang pembuatan system.

e. Bab V UJI COBA DAN EVALUASI

Pada bab ini, menjelaskan implementasi penerapan terhadap system.

f. Bab VI PENUTUP

Berisi kesimpulan yang dapat diambil dari Tugas Akhir ini beserta saran untuk pengembangan selanjutnya.